ANNEX 1: RSA KEYS VERSUS FACTORING

GOULNARA ARZHANTSEVA

We present a proof of a theorem from the second lecture (Chapter 2 of slides). Recall that $n = pq$, where p and q are two distinct k-bit primes.

Reminder:

BPP = if a problem instance x is solvable by a polynomial probabilistic algorithm.

Factoring = given a natural number n compute a prime factor of it.

Asymmetry = compute the private key from the public key.

Asymmetry of RSA = compute d (and not, in addition, p and q), knowing (n, e).

Factoring is not in BPP = there exists no probabilistic polynomial-time algorithm that, given n, finds a non-trivial factor of n with non-negligible probability in k.

Theorem 1. *If the Factoring is not in BPP, then the Asymmetry of RSA is not in BPP.*

Proof. We use the following notation: $\mathbb{Z}/k\mathbb{Z} = \mathbb{Z}_k$ denotes the ring of integers $\bmod k$, $(\mathbb{Z}/k\mathbb{Z})^\times = \mathbb{Z}_k^\times$ denotes the multiplicative group of integers $\bmod k$ and $\mathrm{ord}_k^+ g$ denotes the (additive) order of an element $g \in (\mathbb{Z}_k, +)$, $\mathrm{ord}_k g$ denotes the (multiplicative) order of an element $g \in \mathbb{Z}_k^\times$.

Suppose that the secret key d is computable in polynomial time by a probabilistic algorithm. Our goal is to show that we can factor n, knowing the secret key d and the public key e. By the Chinese Remainder theorem we have an isomorphism[1]:

$$\mathbb{Z}_n^\times \to \mathbb{Z}_p^\times \times \mathbb{Z}_q^\times, a \bmod n \mapsto (a \bmod p, a \bmod q)$$

It follows that

$$\mathrm{ord}_n(a) = \mathrm{lcm}\,(\mathrm{ord}_p(a), \mathrm{ord}_q(a)).$$

Therefore, to factor n we can use the following equivalence (whence p will be a factor):

$$c \equiv 1 \bmod p, c \not\equiv 1 \bmod q \iff n > \gcd(c-1, n) = p > 1.$$

Our goal is to construct such an element c. For an arbitrary element a we have:

$$\begin{aligned} &\mathrm{ord}_p(a) \mid p-1, \\ &\mathrm{ord}_q(a) \mid q-1, \\ &\mathrm{ord}_n(a) \mid (p-1)(q-1) = \phi(n) \mid ed-1 \end{aligned}$$

If we write $ed - 1 = 2^s t$ with some s and with t odd, then $(a^t)^{2^s} = 1$ in the group $\mathbb{Z}_n^\times$ (this group has cardinality $\phi(n)$), hence $\mathrm{ord}_n(a^t) \mid 2^s$. Choose *randomly* an element $a \in \mathbb{Z}_n^\times$ and take $b = a^t$. Then

$$\mathrm{ord}_p(b) = 2^i \text{ and } \mathrm{ord}_q(b) = 2^j \text{ with } i, j \leqslant s.$$

If $i \neq j$, say $i < j$, then we take $c = b^{2^i} \equiv 1 \bmod p$ and $c \not\equiv 1 \bmod q$ and we can factor n by p:

$$p = \gcd(c-1, n).$$

[1] Since the corresponding rings are isomorphic, so are their multiplicative groups. Also, the multiplicative group of a direct product is the direct product of the multiplicative groups.

It remains to show the following claim. Indeed, it will mean that almost every $a \in \mathbb{Z}_n^\times$ has the required property $\mathrm{ord}_p(a^t) \neq \mathrm{ord}_q(a^t)$, see Remark below.

Claim. $i \neq j$ for at least half of all $a \in \mathbb{Z}_n^\times$.

We will use the additive groups $(\mathbb{Z}_k, +)$ to check the Claim, using the isomorphisms:

$$\mathbb{Z}_n^\times \cong \mathbb{Z}_p^\times \times \mathbb{Z}_q^\times \cong (\mathbb{Z}_{p-1}, +) \times (\mathbb{Z}_{q-1}, +),$$

where for a primitive element $g \in \mathbb{Z}_p^\times$, the isomorphism $(\mathbb{Z}_{p-1}, +) \to \mathbb{Z}_p^\times$ is given by $x \mapsto g^x$. The above information on the orders of elements 'translates' into:

$$\mathrm{ord}^+_{p-1}(1) = p - 1 \mid 2^s t \text{ and } \mathrm{ord}^+_{p-1}(t) \mid 2^s.$$

Therefore, our new goal is to show that $\mathrm{ord}^+_{p-1}(xt) \neq \mathrm{ord}^+_{q-1}(yt)$ for at least half of all pairs $(x, y) \in (\mathbb{Z}_{p-1}, +) \times (\mathbb{Z}_{q-1}, +)$.

Let $\mathrm{ord}^+_{p-1}(t) = 2^k$ and $\mathrm{ord}^+_{q-1}(t) = 2^\ell$. Observe[2] that

$$\begin{aligned} \mathrm{ord}^+_{p-1}(t) &= \mathrm{ord}^+_{p-1}(xt) \quad \text{for all } x \text{ odd}, \\ \mathrm{ord}^+_{p-1}(t) &> \mathrm{ord}^+_{p-1}(xt) \quad \text{for all } x \text{ even}. \end{aligned}$$

The same holds if we replace in the above x by y and $p-1$ by $q-1$.

We have two cases.

If $k \neq \ell$, say $\ell < k$, then for all (x, y) with x odd we obtain:

$$\mathrm{ord}^+_{q-1}(yt) \leqslant \mathrm{ord}^+_{q-1}(t) = 2^\ell < 2^k = \mathrm{ord}^+_{p-1}(t) = \mathrm{ord}^+_{p-1}(xt).$$

This strict inequality holds for at least half of the pairs (x, y), namely those with odd x.

If $k = \ell$ then we have two sub-cases:

If x is odd and y is even, then

$$\mathrm{ord}^+_{q-1}(yt) < \mathrm{ord}^+_{q-1}(t) = 2^k = 2^\ell = \mathrm{ord}^+_{p-1}(t) = \mathrm{ord}^+_{p-1}(xt).$$

If x is even and y is odd, then

$$\mathrm{ord}^+_{q-1}(yt) = \mathrm{ord}^+_{q-1}(t) = 2^k = 2^\ell = \mathrm{ord}^+_{p-1}(t) > \mathrm{ord}^+_{p-1}(xt).$$

This strict inequality holds for at least half of pairs (x, y), namely those where $x \not\equiv y \bmod 2$. □

Remark. We use **Erdös' probabilistic method**: if one wants to prove that a structure with certain desired properties exists, one defines an appropriate probability space of structures and then shows that the desired properties hold in this space with strictly positive probability.

The reasoning involves probability but the outcome, that is, the existence of the required structure is certain. The method is *non-constructive*: it does not provide a deterministic algorithm to produce such a required structure. However, it can be used to produce effectively a structure which is very likely with the desired properties (it suffices to choose a random structure).

For example, our proof above shows that a randomly picked $a \in \mathbb{Z}_n^\times$ has the desired property $\mathrm{ord}_p(a^t) \neq \mathrm{ord}_q(a^t)$ with probability $\geqslant 1/2$. Therefore, such $a \in \mathbb{Z}_n^\times$ does exist. Moreover, given a number $r > 0$, picking random $a_1, a_2, \ldots, a_r \in \mathbb{Z}_n^\times$ independently gives $a \in \mathbb{Z}_n^\times$ with the desired property with probability $\geqslant 1-(1/2)^r$ (and the probability of the failure $\leqslant (1/2)^r$). Hence, choosing r to be a polynomial in the bit-length of the input (which is made of (n, e) here) we can make the probability of success exponentially close to 1.

The following theorem (also from Chapter 2 of slides) has an analogous formulation.

Theorem 2. *If the DLP in $\mathbb{Z}_p^\times$ is not in BPP, then the Asymmetry of ElGamal is not in BPP.*

Test question: What is the proof in this case?

[2]Check this!